

Amendments to the Claims

The following listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. Cancelled.
2. Cancelled.
3. Cancelled.
4. Cancelled
5. Cancelled.

6. (currently amended) ~~The method of claim 3~~

A method for conducting authenticated business transactions involving communications using microprocessor equipped devices to communicate over a distributed network, the method being carried out by an on-line authentication service available on the distributed network, comprising the acts of:

- a) enrolling a multiplicity of users with a closed authentication infrastructure, wherein enrolling comprises obtaining and verifying the identity and other credentials of the multiplicity of users and providing each user with a unique secret necessary for later authentication to said on-line authentication service and storing the verified identity and other credentials in at least one database;
- b) authenticating a plurality of the multiplicity of users to said on-line authentication service using each user's unique secret to produce a plurality of authenticated users;
- c) enabling a plurality of groups each group comprising at least two of said plurality of authenticated users to conduct interactions comprising a

plurality of messages under persistent mediation of said on-line authentication service, such that each of the plurality of messages pass through said on-line authentication service and is directly monitored by said on-line authentication service;

- d) wherein persistent mediation of an interaction comprises the acts of directly compiling an audit trail of an interaction and making the audit trail optionally available to the at least two users in the interaction during the interaction at their option; and
- e) further comprising the act of providing a discovery portal available to authenticated users through the on-line authentication service such that users can search for other users based on their verified and unverified credentials, whereby users may conduct authenticated interactions with each other without having a prior relationship.

7.(previously presented)The method of claim 6, wherein the method further comprises the act of enabling the plurality of authenticated users to interact with each other in collaboration groups through the on-line authentication service when a collaboration group comprises at least two users each using a browser operated computing device.

8.(currently amended)The method of claim 7 wherein the act of enabling the plurality of authenticated users to interact with each other in collaboration groups further comprises enabling the at least two users in a collaboration group to make a selection during the interaction of at least part of the audit trail for archival by the on-line authentication service such that it will be held under ~~control~~ of the control of the on-line authentication service for access by any of the at least two users in the interaction after the interaction is complete.

9. (previously presented)The method of claim 6, further comprising the act of accepting dynamically variable credentials from at least some of the plurality of authenticated users, and wherein the act of providing a discovery portal further

comprises the act of providing the plurality of users with the capability of searching for other users based on dynamically variable credentials.

10. (currently amended)The method of claim 7, wherein the collaboration group comprising at least two users each using a browser operated computing ~~devices~~ device comprises greater than two users each using a browser operated computer device.

11. Cancelled.

12. (currently amended)~~The method of claim 11~~

A method for conducting authenticated business transactions involving communications using microprocessor equipped devices to communicate over a distributed network, the method being carried out by an on-line persistent authentication and mediation service available on the distributed network, comprising the acts of:

- a) enrolling users seeking enrollment in the persistent authentication and mediation service, to produce a multiplicity of enrolled users, wherein enrolling comprises obtaining and verifying the identity and other credentials of the multiplicity of users and providing each user with a unique secret necessary for later authentication to said on-line persistent authentication and mediation service;
- b) storing the verified identity and other credentials in at-least one database;
- c) receiving on-line requests from enrolled users for authentication to the on-line authentication service;
- d) authenticating enrolled users seeking authentication to the persistent authentication and mediation service using each enrolled user's secret information, so as to maintain a plurality of authenticated users;
- e) receiving requests from authenticated users to be connected to particular other authenticated users;

- f) connecting groups of at least two authenticated users under persistent mediation of the persistent authentication and mediation service and enabling the at least two authenticated users which are connected to conduct an interaction comprising a plurality of messages;
- g) repeating act (f) to produce a plurality of groups of connected users;
- h) mediating the interaction among the at least two users of each of said plurality of groups of connected users such that each message in the interaction passes through the persistent authentication and mediation service;
- i) directly compiling an audit trail of the interaction and making information from the audit trail available to the at least two users of each group of connected users in intelligible form during the interaction[.]; and
- j) wherein the act of enrolling users seeking enrollment in the persistent authentication and mediation service comprises the acts of:
 - [[a]]i) distributing software to a user seeking enrollment which enables microprocessor equipped devices operated by the user seeking enrollment to interact with said persistent authentication and mediation service,
 - [[b]]ii) generating a unique private key, and a unique public key for the user seeking enrollment,
 - [[c]]iii) obtaining permanent credentials particular to each of the user seeking enrollment, said credentials comprising public permanent credentials and secret permanent credentials,
 - [[d]]iv) deciding whether to approve the applicant seeking enrollment;
 - [[e]]v) distributing the unique secret comprising a camouflaged private encryption key to the user seeking enrollment if the user seeking enrollment is approved, wherein the private key is camouflaged in a software container, whereby the user's camouflaged private key will generate a correct response to an authentication challenge if a proper access code is entered, but often generates an incorrect but plausible response if an improper access code is entered, whereby if an incorrect

response is used notice will be provided to the on-line persistent authentication and mediation service of a security attack;

[[f]]vi) distributing a unique public key to the user, wherein said public key can only be decrypted with a key held under exclusive control of the persistent authentication and mediation service, whereby the persistent authentication and mediation service acts as a closed authentication infrastructure;

[[g]]vii) storing said permanent credentials in a customer database, said customer database being accessible to said persistent authentication and mediation service, whereby the user seeking enrollment becomes one of said multiplicity of enrolled users; and

[[h]]viii) repeating steps [[(a)]]1) through [[(f)]vi] for each applicant seeking enrollment.

13. (previously presented) The method of claim 12 wherein the act of authenticating enrolled users seeking authentication to the persistent authentication and mediation service comprises the acts of:

- a) generating a challenge message and sending it over the public network to an enrolled user seeking authentication,
- b) receiving a response to the challenge from the user seeking authentication, said response comprising an encrypted message and the encrypted unique public key of the enrolled user seeking authentication,
- c) verifying the authenticity of the response to the challenge, the act of verifying the authenticity comprising the act of decrypting the unique public key and then decrypting the response using the unique public key of the enrolled user seeking authentication to produce a decrypted response,
- d) authenticating the enrolled user seeking authentication if the decrypted response indicates that the response was authentic, whereby the enrolled user seeking authentication becomes an authenticated user,
- e) rejecting the user if the decrypted response indicates that the response was not authentic, and

- f) repeating steps (a) through (e) for each enrolled user seeking authentication.

14. (currently amended)The method of claim [[11]]13 further comprising the acts of:

- a) allowing authenticated users to optionally submit variable credentials;
- b) receiving variable credentials submitted by authenticated users;
- c) storing the variable credentials in the customer database according to user;
- d) providing authenticated users discovery software, whereby authenticated users may dynamically discover enrolled users according to search criteria[.]; and
- e) granting authenticated users access to search the public permanent credentials and the variable credentials in the customer database, using said discovery software.

15.(original)The method of claim 14 further comprising making available collaboration software to each of said plurality of groups of connected users to facilitate communication among the at least two authenticated users of each group, wherein said collaboration software makes information from the audit trail available to each of said at least two authenticated users of each of said plurality of groups of connected users.

16.(currently amended)The method of claim 15 wherein:

- a) the unique secret comprises a cryptographically camouflaged private key in a software container[.];
- b) wherein the unique public key[[s]] is encrypted with a key held under the exclusive control of the persistent authentication and mediation service and stored in a digital certificate[.]; and
- c) wherein the act of authenticating an enrolled user to the ~~common~~ authenticating persistent authentication and mediation service further comprises the act of decrypting the encrypted unique public key unique to the enrolled user prior to decrypting the response.

17. (currently amended)The method of claim 14 wherein the persistent authentication and mediation service is provided by at least one host site connected to the distributed network, said at least one host site comprising at least one computer server operated by an open software platform providing intelligent interactions, wherein the operation of the persistent authentication and mediation service is implemented by software operating on the open software platform.
- 18.(original)The method of claim 17 wherein interactions between users and the persistent authentication and mediation service are mediated through the open software platform.
- 19.(original)The method of claim 18 wherein some of the plurality of groups of connected users comprise at least three authenticated users.
- 20.(original)The method of claim 19 wherein some of the plurality of groups of at least three connected users comprise users of different types.
- 21.(original)The method of claim 18 wherein the distributed network is the public Internet.
22. (original)An online service for conducting business transactions among microprocessor equipped devices over a distributed network, the online service comprising:
- a) a host site connected to the network, the host site comprising an open software platform providing intelligent interactions;
 - b) a persistent authentication and mediation service, the persistent authentication and mediation service comprising a software PKI authentication agent operating on said open software platform such that communications over the network by said persistent authentication and mediation service are mediated by said open software platform;

- c) a customer database comprising permanent credentials and dynamically variable information corresponding to users of the online service and a database manager for managing the customer database;
- d) software operating on said open software platform which performs at least the following functions:
 - i) enrolling users seeking enrollment in the persistent authentication and mediation service to produce enrolled users,
 - ii) storing credentials corresponding to enrolled users in the customer data base,
 - iii) authenticating enrolled users seeking authentication to the persistent authentication and mediation service to produce authenticated users,
 - iv) allowing [[a]] authenticated users to discover enrolled users according to search criteria,
 - v) allowing authenticated users to be connected under mediation of the persistent authentication and mediation service through the open software platform,
 - vi) allowing collaboration between authenticated users which have been connected, and
 - vii) memorializing transactions between authenticated users.

23. (currently amended)The online service defined in claim 22 where the function of enrolling users seeking enrollment in the persistent authentication and mediation service comprises the functions of:

- a) distributing software to a user seeking enrollment which enables microprocessor equipped devices operated by the user seeking enrollment to interact with the persistent authentication and mediation service,
- b) generating a unique private key, and a unique public key for the user seeking enrollment,

- c) obtaining permanent credentials particular to each of the user seeking enrollment, said credentials comprising public permanent credentials and secret permanent credentials,
- d) deciding whether to approve the applicant seeking enrollment[[;]],
- e) distributing the unique public key and the unique private key to the user seeking enrollment if the user seeking enrollment is approved, [[and]]
- f) storing said permanent credentials in a customer database, said customer database being accessible to said persistent authentication and mediation service, whereby the user seeking enrollment becomes one of [[said]]a multiplicity of enrolled users, and
- g) repeating steps (a) through (f) for each applicant seeking enrollment.

24. (original)The online service defined in claim 23 wherein the function of authenticating enrolled users seeking authentication to the persistent authentication and mediation service comprises the functions of:

- a) generating a challenge message from the persistent authentication and mediation service and sending it over the public network to an enrolled user seeking authentication,
- b) receiving a response to the challenge from the user seeking authentication, said response comprising an encrypted message and the unique public key unique to the enrolled user seeking authentication,
- c) verifying the authenticity of the response to the challenge, the act of verifying the authenticity comprising the act of decrypting the response using the public key unique to the enrolled user seeking authentication to produce a decrypted response,
- d) authenticating the enrolled user seeking authentication if the decrypted response indicates that the response was authentic, whereby the enrolled user seeking authentication becomes an authenticated user,
- e) rejecting the user if the decrypted response indicates that the response was not authentic, and

- f) repeating steps (a) through (e) for each enrolled user seeking authentication.

25. (currently amended)The online service defined in claim 24 wherein:

- a) the software PKI authentication agent is a pseudo-PKI system of the type which cryptographically camouflages each of the unique private keys in a software container,
- b) wherein each of the unique public keys is encrypted in a form recognizable to the pseudo-PKI authentication agent and stored in a digital certificate, and
- c) wherein the function of authenticating an enrolled user to the persistent authentication and mediation service further comprises the function of decrypting the encrypted unique public key unique to the enrolled user prior to decrypting the response.

26. (previously presented)The online service defined in claim 22 wherein the distributed network is the public Internet.

27.(currently amended)A system for conducting business transactions over a distributed network, the system comprising:

- a) a persistent authentication and mediation service site providing a persistent authentication and mediation service, said site connected to the public network, said site comprising
 - i) an open software platform application providing intelligent interactions said platform application mediating all interactions of said persistent authentication and mediation service site via said public network,
 - ii) an authentication agent application comprising a software pseudo-PKI authentication application operating on said open software platform application, said authentication agent application comprising software which enrolls new business[[es]] users

- producing enrolled users and authenticates the enrolled users
producing authenticated business users,
- iii) an audit agent application operating on said open software platform which logs and monitors interactions mediated by the open software platform, whereby every interaction among authenticated business users passes through the open software platform and is monitored by the audit agent,
 - iv) a discovery software application operating on said open software platform such that said discovery software agent operates to enable authenticated business users to search for other users based on their credentials, and
 - v) a collaboration software application operating on said open software wherein said collaboration software application enables groups of at least two authenticated business users to communicate under direct mediation of the audit agent and to access audit information in an intelligible form during an interaction[.];
- b) a multiplicity of user sites operated by the enrolled users, the user sites being connected to the public network, each site operating at least one computer application whereby it may interact with other business users and each site further comprising software which allows interaction with the persistent authentication and mediation service, a software camouflaged private key, and a digital certificate, said digital certificate comprising an encrypted pseudo-public key encrypted with a key which is under exclusive control of said persistent authentication and mediation service, wherein said camouflaged private key will generate a proper response to a challenge from the persistent authentication and mediation service if a correct access code is entered and may generate plausible but improper responses if incorrect access codes are entered, whereby if an incorrect response is used the persistent authentication and mediation service will be alerted to a security attack on the camouflaged private key; and

- c) a database of authentication information and credentials pertaining to the enrolled business users of said persistent authentication and mediation service, the database accessible to the authentication agent application and the discovery application.

28.(original) The system defined in claim 27 further comprising a plurality of authentication provider applications accessible by the authentication agent application.

29. (previously presented)The system defined in claim 27 wherein at least one authentication provider application is located at a different site than the persistent authentication and mediation service site.

30. (previously presented)The system defined in claim 27 further comprising a plurality of audit provider applications accessible by the audit agent application.

31. (previously presented)The system defined in claim 27 wherein at least one authentication application provider is located at a different site than the persistent authentication and mediation service site.

32. Cancelled.

33. (previously presented)The system defined in claim 27 wherein the network is the public Internet.

34. (previously presented)The system defined in claim 27, wherein the user sites comprise sites which are chosen from the group consisting of user sites which access the network via a browser operating on a computer, mobile telephonic devices which access the network, world wide web sites, and sites comprising applications without a user interface.

35.(currently amended)An apparatus for providing a service for conducting authenticated business transactions involving a multiplicity of users over a distributed network, the apparatus comprising:

- a) at least one application server connected to the public network, the at least one application server having a computer processor and a computer readable memory, the memory storing the software to implement the service, the software comprising
 - i) an open software platform providing intelligent interactions,
 - ii) a software pseudo-PKI authentication agent application, operating on said open software platform,
 - iii) a discovery software application, operating on said open software platform, and
 - iv) a collaboration software application, operating on said open software platform[[,]];
 - b) at least one database server, the at least one database server comprising a business users database, the business users database comprising
 - i) authenticated data about registered business users, said authenticated data being protected from user modification;
 - ii) data pertaining to registered business users which is dynamically modifiable by said business users; and
 - iii) data needed for linking business users;
- whereby the application server facilitates authenticated interactions between business users, including the ability to access other authenticated users without repeated logging in, the ability to dynamically search for authenticated users according to user defined specifications, and accomplish peer to peer collaboration.

36. (currently amended)The apparatus as defined in claim 35 where the distributed network is the public Internet.